UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/769,103	01/30/2004	Daniel M. Bodorin	MSFT122222	9005

26389 7590 10/30/2007
CHRISTENSEN, O'CONNOR, JOHNSON, KINDNESS, PLLC
1420 FIFTH AVENUE
SUITE 2800
SEATTLE, WA 98101-2347

EXAMINER	
HAILU, TESHOME	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
10/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

mv

Office Action Summary	**Application No.** 10/769,103	**Applicant(s)** BODORIN ET AL.
	Examiner Teshome Hailu	**Art Unit** 2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6* is/are pending in the application.

4a) Of the above claim(s) *2,3,5 and 6* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 4* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 January 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)	4) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) □ Notice of Informal Patent Application
3) □ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.	6) □ Other: _____.

DETAILED ACTION

1. Claims 1-6 are pending.

2. Claims 2,3,5 and 6 are withdrawn form consideration.

3. Claims 1 and 4 are rejected.

Election/Restrictions

4. Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1 and 4, are drawn to a system and method of detecting a malware, classified in class 726, subclass 24.

II. Claims 2, 3, 5 and 6, are drawn to a system and method of unpacking a packed executable, classified in class 717, subclass 120.

5. Inventions I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct if they don not overlap in scope and are not obvious variants, and if it is shown that at least one subcombination is separately usable. In the instant case, the system and method of detecting a malware in subcombination I can be utilized in virus detection of an executable, while the system and method of unpacking packed executable in subcombination II is utilized in software management. See MPEP 806.05(d).

Because these inventions are independent or distinct for the reasons given above and have acquired a separate status in the art in view of their different classification, restriction for examination purpose as indicated is proper.

Applicant is advised that the reply to this requirement to be complete must include (i) an election of a species or invention to be examined even though the requirement be traversed (37 CFR 1.143) and (ii) identification of the claims encompassing the elected invention.

The election of an invention or species may be made with or without traverse. To reserve a right to petition, the election must be made with traverse. If the reply does not distinctly and specifically point out supposed errors in the restriction requirement, the election shall be treated as an election without traverse. Should the applicant traverse on the ground that the inventions or species are not patentably distinct, applicant should submit evidence or identify such evidence now of record showing the inventions or species to be obvious variants or clearly admit on the record that this is the case. In either instance, if the examiner finds one of the inventions unpatentable over prior art, the evidence or admission may be used in a rejection under 35 U.S.C 103(a) of the other invention.

6. During a telephone conversation with Tracy S. Powell on 19 October 2007 a provisional election was made without traverse to prosecute the invention of Group I, claims 1 and 4. Affirmation of this election must be made by applicant in replying to this Office action. Claims 2, 3, 5 and 6 are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1 and 4 are rejected under 35 U.S.C. 102(e) as being anticipated by Lucas et al (Lucas), US 6,968,461.

As per claim 1, Lucas discloses:

A system for determining whether a packed executable is malware, the system comprising: (column 3, line 63-64, "FIG. 2 illustrates virus scanning operation when access is made to a compressed computer file 18").

A malware evaluator for determining whether incoming data is malware; (column 3, line 55-59," Within the anti-virus system 12 an anti-virus engine 14 working with virus definition data 16 serves to apply a plurality of tests for different known viruses and virus like behavior to the computer file in order to detect the presence of a computer virus within that computer file").

An unpacking module that receives a packed executable from the malware evaluator and returns an unpacked executable corresponding to the packed executable; (column3, line 63-67 and column 4, line 1-2, "FIG. 2 illustrates virus scanning operation when access is made to a compressed computer file 18. In order that this compressed computer file 18 can be properly checked it is decompressed into an uncompressed file form 20 and then a sequence of tests corresponding to separate DAT driver files within the virus definition data 16 are applied to the uncompressed data").

Wherein the malware evaluator, upon receiving incoming data, determines whether the incoming data is a packed executable, and if so, provides the packed executable to the unpacking module and receives from the unpacking module an unpacked executable, and determines whether the unpacked executable is malware. (Column 4, line 2-6, "In practice the anti-virus system 12 requests a portion of the compressed file 18 to be decompressed and then applies the tests to that decompressed portion. If further portions still requiring checking, then more of the compressed file is decompressed and checked").

As per claim 4, Lucas discloses:

A method for determining whether incoming data is malware, the method comprising: (column 1, line 7-9, "This invention relates to the field of data processing systems. More particularly, this invention relates to the field of the detection of computer viruses within computer files").

Intercepting incoming data directed to a computing device; (column 3, line 51- 54, "This operating system file system 8, prior to servicing the access request from an associated hard disk drive 10, generates a scan request that is passed to an anti-virus system 12 together with the file concerned and further associated data"). The file passes through the anti-virus means the anti-virus system intercept the file prior to getting in hard disk.

Determining whether the incoming data is a packed executable; and if the incoming data is a packed executable:. generating an unpacked executable, the unpacked executable corresponding to the packed executable; (column 4, line 22-26, "At step 24, a determination is made as to whether or not the portion of data recovered from the computer file being scanned requires decompressing or unpacking prior to testing. If the data does require decompressing or unpacking, then this is performed at step 26"). Where step 26 is a step of decompressing or unpacking a data. See fig. 3.

Determining whether the packed executable is malware by evaluating whether the unpacked executable is malware. (Column 4, line 2-6, "In practice the anti-virus system 12 requests a portion of the compressed file 18 to be decompressed and then applies the tests to that decompressed portion. If further portions still requiring checking, then more of the compressed file is decompressed and checked").

Conclusion

1. The prior art made or record and not relied upon is considered pertinent to applicant's disclosure

TITLE: Apparatus, methods and computer programs for identifying or managing vulnerabilities within a data processing network, US Pub. No. 2005/0132206.

TITLE: Detecting computer programs within packed computer files, US Pub. No. 2003/0023865.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Teshome Hailu whose telephone number is (571) 270-3159. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m. PST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Teshome Hailu

October 23, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100